Logické systémy

Proč mluvit o logických systémech

* Co je logické uvažování, matematicky?
  Kde jsou jeho limit?
  Dá se mechanizovat?
* ***Logický systém*** matematicky přesně definuje
  - co je logických výrok, jaký je jeho význam (syntax a sémantika),
  - co je logická argumentace (důkaz).

Odvozovací (deduktivní) systém

* Definuje, co je logická argumentace, důkaz.
* Skládá se z
  * axiomů, základních zjevný pravd, a
  * odvozovacích (deduktivních) pravidel.
* Důkaz je sekvencí použití deduktivních pravidel, vycházející z axiomů.

Část I

Systém výrokové logiky

Deduktivní systém výrokové logiky

* ***Schémata výrokových axiomů***

$$
\begin{array}{ll}
\text{(A1)} & A \to (B \to A) \\
\text{(A2)} & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\
\text{(A3)} & (\neg B \to \neg A) \to ((\neg B \to A) \to B)
\end{array}
$$

kde A, B, C jsou libovolné výrokové formule.

* ***Odvozovací pravidlo modus ponens (pravidlo odloučení)***

(MP) Z *předpokladů* A a $(A \to B)$ odvodíme *závěr* B.

* (A1): Pokud A určitě platí a dovím se B, tak A bude pořád platit.
* (A2): V podstatě tranzitivita implikace.
* (A3): Pokud z výroku $(\neg B)$ plyne spor, pak neplatí. Tedy platí opak (B).
* (MP): Z (*prší* $\to$ *nemám deštník*) a *prší* odvodím, že *nemám deštník*.

Důkaz

Důkaz formule φ
je sekvence formulí $\varphi_1, \ldots, \varphi_n$, kde $\varphi_n = \varphi$ a pro každé $i : 1 \leq i \leq n$, formule φ_i je axiomem nebo vznikla z $\varphi_1, \ldots \varphi_{i-1}$ aplikací odvozovacích pravidel.

Pokud existuje důkaz φ, tak je φ ***dokazatelná***, psáno $\vdash \boldsymbol{\varphi}$.

Důkaz z předpokladů

Důkaz formule φ ***z množiny předpokladů*** T,
kde T je množina formulí,
je sekvencí formulí $\varphi_1, \ldots, \varphi_n$, kde $\varphi_n = \varphi$ a pro každé $i : 1 \leq i \leq n$,
formule φ_i je axiomem nebo prvkem T
nebo vznikla z $\varphi_1, \ldots \varphi_{i-1}$ aplikací odvozovacích pravidel. Píšeme $\boldsymbol{T} \vdash \boldsymbol{\varphi}$.

Příklad důkazu: $\vdash A \to A$

$$
\begin{array}{lll}
(1) & A \to ((A \to A) \to A) & \text{(A1)} \\
(2) & (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) & \text{(A2)} \\
(3) & (A \to (A \to A)) \to (A \to A) & \text{(1),(2) MP} \\
(4) & A \to (A \to A) & \text{(A1)} \\
(5) & A \to A & \text{(3),(4) MP}
\end{array}
$$

Pozn.:

(1) je (A1) pro volbu A, $A \to A$ za A, B

(2) je (A2) pro volbu A, $A \to A$, A za A, B, C

(3) je závěr MP z předpokladů (1), (2)

Část II

Systém predikátové logiky

Axiomy PL

* ***Schémata výrokových axiomů***

$$\begin{array}{ll} \text{(A1)} & \varphi \to (\psi \to \varphi) \\ \text{(A2)} & (\varphi \to (\psi \to \eta)) \to ((\varphi \to \psi) \to (\varphi \to \eta)) \\ \text{(A3)} & (\neg\psi \to \neg\varphi) \to ((\neg\psi \to \varphi) \to \psi) \end{array}$$

  kde φ, ψ, η jsou formule PL.

* ***Schéma axiomů kvantifikátoru***: Není-li x volné ve φ, pak

$$(\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x \psi))$$

* ***Schéma axiomů substituce***:

$$(\forall x\, \varphi) \to \varphi[x/t]$$

  kde t je term substituovatelný za x do φ.

Axiomy PL

- Pokud pracujeme s jazykem s rovností, přidáváme ***axiomy rovnosti***:
  Pro libovolné funkční a predikátové symboly f/n a p/n a proměnné $x, x_1, \dots, x_n, y_1, \dots, y_n$

$$x = x$$

$$x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow (\dots(x_n = y_n \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n))\dots))$$

$$x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow (\dots(x_n = y_n \rightarrow p(x_1, \dots, x_n) \rightarrow p(y_1, \dots, y_n))\dots))$$

Příklady axiomů PL

* axiom kvantifikátoru: $(\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x \psi))$

$$(\forall \mathit{Brňák}\ (\mathit{je\ hezky} \to \mathit{Brňák\ je\ na\ přehradě})) \to \\ (\mathit{je\ hezky} \to (\forall \mathit{Brňák}(\mathit{Brňák\ je\ na\ přehradě})))$$

* axiom substituce: $(\forall x\, \varphi) \to \varphi[x/t]$

$$(\forall x\, x < \infty) \to (5 + 5 < \infty)$$

* ax. rovnosti: $x_1 = y_1 \to (\ldots(x_n = y_n \to p(x_1, \ldots, x_n) = p(y_1, \ldots, y_n))\ldots)$

$$(\mathit{pivo} = \mathit{chleba} \to (\mathit{snídaně}(\mathit{chleba}, \mathit{máslo}) \to \mathit{snídaně}(\mathit{pivo}, \mathit{máslo}))$$

Odvozovací pravidla predikátové logiky

* ***Modus ponens***:

  Z předpokladů φ a $(\varphi \to \psi)$ odvodíme závěr ψ.

* ***Pravidlo zobecnění (generalizace)***:

  Z předpokladu φ odvodíme závěr $(\forall x \varphi)$.

Např., platí-li $x < \infty$, potom platí $(\forall x\, x < \infty)$.

Příklad důkazu v PL: $p(x, y) \vdash p(y, x)$

(1)	$p(x, y)$	(předpoklad)
(2)	$\forall y\, p(x, y)$	(pravidlo zobecnění)
(3)	$\forall x \forall y\, p(x, y)$	(pravidlo zobecnění)
(4)	$(\forall x \forall y\, p(x, y)) \rightarrow (\forall y\, p(z, y))$	(axiom substituce, x za z)
(5)	$\forall y\, p(z, y)$	(MP)
(6)	$(\forall y\, p(z,y)) \rightarrow p(z,x)$	(axiom substituce, y za x)
(7)	$p(z, x)$	(MP)
(8)	$(\forall z\, p(z, x))$	(pravidlo zobecnění)
(9)	$(\forall z\, p(z, x)) \rightarrow p(y, x)$	(axiom substituce, z za y)
(10)	$p(y, x)$	(MP)

Pozn.:
(1): předpoklad; (2): p. zobec. pro $\varphi = (1)$, x = y; (3): p. zobec. pro $\varphi = (2)$;
(4): ax. subst. pro $\varphi = (3)$ a $t = z$; (5): MP pro $\varphi = (3)$ a $\varphi \rightarrow \psi = (4)$;
(6): ax. subst. pro $\varphi = (5)$, $x = y$ a $t = x$; (7): MP pro $\varphi = (5)$ a $\varphi \rightarrow \psi = (6)$;
(8): ax. subst. pro $\varphi = (7)$, $x = z$; (9): ax. subst. pro $\varphi = (8)$, $x = z$ a $t = y$;
(10): MP pro $\varphi = (8)$ a $\varphi \rightarrow \psi = (9)$;

Formlání důkaz versus běžný důkaz

* Formální logický systém je jakýsi „asembler“ logického odvozování.
  - Důkaz je absolutně nezpochybnitelný, mechanicky zkontrolovatelný.
  - Proto je formální odvozování extrémně detailní, mechanicky jednoduché, a systém je minimalistický.
  - Formální systém je stavěn tak, aby se dobře přemýšlelo *o něm*, ne *v něm*.
* Běžný důkaz je poloformální.
  - Čtenář by měl snadno pochopit a zároveň nepochybovat.
  - Dělají se větší kroky, spoléhá se na čtenářovu intuici a znalosti.
  - Je expandovatelný na plně formální důkaz.

K zapamatování

- Logický systém
- Deduktivní (odvozovací, důkazový) systém.
- Axiom
- Odvozovací pravidlo
- Důkaz
- Důkaz z předpokladů

Část III

Vlastnosti logických systémů

Ideál logických systémů

* Ideálem je logický systém, pomocí kterého můžeme

  efektivně dokázat nebo vyvrátit všechna zajímavá tvrzení.

  Navíc bychom také dokazování chtěli ***mechanizovat***.


HILBERT
POĎME
NA TO!

Efektivnost

Logický systém je efektivní, pokud můžeme efektivně ověřit korektnost logického argumentu, důkazu. Můžeme pro něj napsat program Ověřovač, který ověří, že daný řetězec symbolů je důkaz.

Výroková i predikátová logika je efektivní.

* Protože můžeme algoritmicky ověřit
  1. co je dobře formulovaná formule,
  2. co je axiom,
  3. že formule v důkazu byla odvozena odvozovacími pravidly z předchozích.

Příklady neefektivních logických systémů

* Axiomy jsou všechna tvrzení, na která nikdy nebudeme znát odpověď.
* Všechny aritmetické vlastnosti platící pro všechna celá čísla jsou axiomy.

Dokazatelnost versus Platnost

$$\vdash \varphi$$

Dokazatelná (z axiomů pomocí odvozovacích pravidel).
Čistě syntaktická manipulace.

$$\models \varphi$$

Platná ve všech interpretacích.
Rozhoduje sémantika (význam).

Ve VL ověříme pravď. tabulkou.
V PL problém s nekon. dom. a $\forall\psi$

$\vdash \varphi$ je ověřením $\models \varphi$
Důkaz je ověřením platnosti.

Mělo byt tedy platit, že
$$\vdash \varphi \iff \models \varphi.$$

Korektnost

Systém je ***korektní*** pokud

$$\vdash \varphi \implies \models \varphi$$

Co je dokazatelné, to je platné.
Nemůžeme dokázat nesmysly.

Úplnost

Systém je ***úplný*** pokud
$$\models \varphi \implies \vdash \varphi$$

Vše platné můžeme dokázat.

Korektnost a úplnost VL a PL

Výroková i predikátová logika je korektní a úplná. (Post, Gödel)

Pro libovolnou formuli VL nebo PL platí $\models \varphi \Longleftrightarrow \vdash \varphi$.

Pro PL je to Gödelova věta o úplnosti.

Kurt Gödel

Brno, 1906 - 1978

K zapamatování

- Efektivnost
- Korektnost
- Úplnost
- Gödelova věta o úplnosti PL (dokazatelné je platné)

Část IV

Prvořádové teorie

Platnost a dokazování ve vybraných strukturách

* $\models \varphi$ je logická platnost formulí jako

$$\models \ \forall x(x > x) \to 1 > 1$$

  Platí pro všechny interpretace $<$ a 1.
* Je následující formule logicky platná?

$$\not\models \ 1 + 1 = 2$$

  Není, neplatí pro všechny interpretace $+$, 1 a 2 (např. $+$ může být násobení).
* Chceme vyjádřit, že $1 + 1 = 2$ je platná v přirozených číslech jak je známe (t.j. když 1, 2, a $+$ jsou interpretovány, jak jsme zvyklí), a chtěli bychom to i dokázat.
* Obecně, ***chtěli bychom formálně definovat mat. struktury a dokazovat, že formule platí v definovaných strukturách***.
* K tomu slouží logické teorie:

Teorie

Teorie s jazykem L je množina uzavřených prvořádových formulí T s jazykem L.
Formulím $\psi \in T$ říkáme ***speciální axiomy*** teorie T.

Teorie definuje matematické struktury:

Model teorie T je realizace $\mathcal{M}$ jazyka L, kde $\mathcal{M} \models \psi$ pro všechny $\psi \in T$.
Píšeme $\boldsymbol{\mathcal{M}} \models \boldsymbol{T}$.

Můžeme pak mluvit o platnosti formule ve strukturách definovaných teorií:

Důsledek teorie je formule φ platná ve všech jejích modelech.
Píšeme $\boldsymbol{T} \models \boldsymbol{\varphi}$.

Dokazování v teoriích

$\boldsymbol{T} \vdash \boldsymbol{\varphi}$, φ je dokazatelná z předpokladů T (viz. slajd 7)

- Můžeme tedy dokazovat platnost ve strukturách definovaných teorií.
- Dohromady je provořádová teorie nový logický systém. Má vlastní sémantiku, danou $T \models$, a vlastní důkazový systém, daný $T \vdash$ (namísto původních $\models$ a $\vdash$).
- Dokazujeme formule platné v mat. strukturách „definovaných“ teorií.

Stále platí Gödelova věta o úplnosti PL:

$$\boldsymbol{T} \models \boldsymbol{\varphi} \Longleftrightarrow \boldsymbol{T} \vdash \boldsymbol{\varphi}$$

Příklady teorií

Teorie ostrého uspořádání $T_<$ má speciální axiomy

$$\begin{aligned} &\forall x(x \not< x) && \text{(ireflexivita)}\\ &\forall x \forall y \forall z((x < y \land y < z) \to x < z) && \text{(tranzitivita)}\\ &\forall x \forall y \forall z((x < y \land y < x) \to x = y) && \text{(slabá antisymtetrie)} \end{aligned}$$

Příklad modelu: $D_{\mathcal{M}} = \{1, 2, 3\}$, $\alpha_{\mathcal{M}}(<) = \{(1, 2), (2, 3), (1, 3)\}$.
$T_< \models x \not< y \lor y \not< x$ (platí pro všechna o. u.) a $T_< \vdash x \not< y \lor y \not< x$ (dokazatelné)

Teorie grup T_G má speciální axiomy

$$\begin{aligned} &\forall x \forall y \forall z(x \cdot (y \cdot z) = (x \cdot y) \cdot z) && \text{(asociativita)}\\ &\forall x(x \cdot e = x \land e \cdot x = x) && \text{(neutrální prvek)}\\ &\forall x \exists y(x \cdot y = e \land y \cdot x = e) && \text{(inverzní prvky)} \end{aligned}$$

Př.: $D_{\mathcal{M}} = \{0, 1\}$, $\alpha_{\mathcal{M}}(.) = \{((0, 0), 0), ((0, 1), 0), ((1, 0), 0), ((1, 1), 1)\}$
$T_G \models x = e \to x \cdot x = x$ a také $T_G \vdash x = e \to x \cdot x = x$.

Příklady teorí: Peanova aritmetika T_{PA}

1. $\forall x \neg(S(x) = 0)$ (nula je první)
2. $\forall xy(S(x) = S(y) \rightarrow x = y)$ (každý má jiného následníka)
3. pro formule φ jazyka T_{PA} s jednou volnou proměnou:

$$\left[\varphi(0) \wedge (\forall x(\varphi(x) \rightarrow \varphi(S(x))))\right] \rightarrow \forall x\,(\varphi(x)) \qquad \text{(ax. indukce)}$$

4. $\forall x(x + 0 = x)$ (0 je neutrální k $+$)
5. $\forall xy(x + S(y) = S(x + y))$ (def sčítání)
6. $\forall x(x \cdot 0 = 0)$ (0 je nulová k $\cdot$)
7. $\forall xy(x \cdot S(y) = x \cdot y + x)$ (def násobení)

$$0, \overset{1}{S(0)}, \overset{2}{S(S(0))}, \overset{3}{S(S(S(0)))}, \overset{4}{S(S(S(S(0))))}, \overset{5}{S(S(S(S(S(0)))))}, \ldots$$

$$T_{PA} \models \overset{1}{S(0)} + \overset{1}{S(0)} = \overset{2}{S(S(0))} \quad \text{a} \quad T_{PA} \vdash \overset{1}{S(0)} + \overset{1}{S(0)} = \overset{2}{S(S(0))}$$

Bezespornost

Teorie T je ***bezesporná***, pokud neexistuje formule φ taková, že $T \vdash \varphi$ a $T \vdash \neg\varphi$.

* Bezespornost je základ smysluplnosti. Axiomy si nesmí protiřečit.
* Ve sporné teorii je možné dokázat cokoliv.
  Pokud $T \vdash \varphi$ a $T \vdash \neg\varphi$, pak i $T \vdash \varphi \wedge \neg\varphi$. Nepravda je tedy dokazatelná.
  Z nepravdy pak plyne cokoliv (protože $0 \rightarrow \psi$ vždy platí).
* Sporná teorie nemůže mít žádný model, protože nepravda nemůže platit v žádné interpretaci.

Teorie je bezesporná právě tehdy, když má model.

Bezespornost, příklad

Teorie T:

$$\forall x \forall y\, (x < y)$$
$$\neg \forall x \forall y\, (x < y)$$
$$\forall x\, (x \not< x)$$

Teorie T':

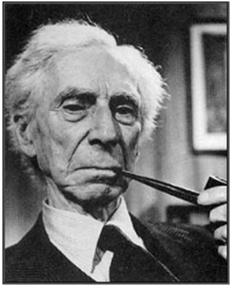
$$\forall x \forall y \forall z\, (x.(y.z)) = ((x.y).z)$$
$$\forall x\, (x.e = e.x = x)$$
$$\exists z\, (z \neq e \wedge \forall x\, (x.z = z.x = x))$$

Teorie T'':

$$\exists x\, (f(x) = 0)$$
$$\forall x \forall y\, (f(x) = f(y))$$
$$\neg \exists x\, (f(x) = x)$$

Slavná sporná teorie: naivní teorie množin

Bertrand Russel



Hmmm hmmmm

Mějme množinu M, obsahující všechny množiny, které nejsou svým vlastním prvkem.
Je M svým vlastním prvkem?
Jestli je M vlastním prvkem, pak, podle definice, není vlastním prvkem.
Jestli M není vlastním prvkem, pak, podle definice, je vlastním prvkem.
Zatr sakr ...

Úplnost teorií, intuitivně

* Úplnost teorie formalizuje „přesnost“, nebo „jednoznačnost“ definice.
* Definice je přesná, jednoznačná, pokud definuje přesně jednu věc, jednu mat strukturu. Nevyhovuje jí hned několik různých mat. struktur.

Úplnost teorií

Teorie T je ***úplná***, pokud pro každou uzavřenou formuli φ jazyka T platí
$T \vdash \varphi$, nebo $T \vdash \neg\varphi$.
(Každou uzav. formuli jazyka je v T možno dokázat nebo vyvrátit.)

* Nechť T má právě jeden model $\mathcal{M}$ (až na izomorfismus).
* Pro každou formuli jazyka T máme $\mathcal{M} \models \varphi$, nebo $\mathcal{M} \models \neg\varphi$ (z def. $\mathcal{M} \models$).
* Protože $\mathcal{M}$ je jediný, tak $T \models \varphi$, nebo $T \models \neg\varphi$.
* Z věty o úplnosti PL ($T \models \psi \Leftrightarrow T \vdash \psi$) plyne, že $T \vdash \varphi$, nebo $T \vdash \neg\varphi$.

Teorie má jediný model $\Rightarrow$ je úplná.

Je úplná $\Leftrightarrow$ nemá dva modely rozlišitelné fomulemi jazyka
(t.j., neexistují $\mathcal{M}, \mathcal{M}', \varphi$ tak, že $\mathcal{M} \models \varphi$ a $\mathcal{M}' \models \neg\varphi$)

Úplnost teorií, příklady

Teorie relací ekvivalence:

$$\forall x\,(x \sim x)$$
$$\forall x \forall y\,(x \sim y \to y \sim x)$$
$$\forall x \forall y \forall z\,((x \sim y \wedge y \sim z) \to x \sim z)$$

* $\mathcal{M}$: $D_{\mathcal{M}} = \{1\}$, $\alpha_{\mathcal{M}}(\sim) = \{(1,1)\}$
* $\mathcal{M}'$: $D_{\mathcal{M}'} = \{1,2\}$, $\alpha_{\mathcal{M}'}(\sim) = \{(1,1),(2,2)\}$
* $\varphi : \forall x \forall y\,(x \sim y)$, $\mathcal{M} \models \varphi$ a $\mathcal{M}' \models \neg\varphi$, tedy není úplná.

Chceme definovat dvouprvkový svaz s maximem 1 a minimem 0.

$$0 < 1 \wedge 0 < 0 \wedge 1 < 1 \wedge 1 \not< 0$$
$$\forall x\,(x = 0 \vee x = 1)$$

$$\mathcal{M} : D_{\mathcal{M}} = \{a,b\}, \alpha_{\mathcal{M}}(<) = \{(a,b),(a,a),(b,b)\},\ \alpha_{\mathcal{M}}(0) = \{a\},\ \alpha_{\mathcal{M}}(1) = \{b\}$$

Jediný model $\Rightarrow$ je úplná.

Příklad (beze)sporné a (ne)úplné teorie

$$\varphi_1 : \exists x \forall y (x.y = y) \qquad \varphi_2 : \exists x \forall y (x.y = x) \qquad \varphi_3 : \neg \exists x (x.x = x)$$

* $T_1 = \{\varphi_1\}$
  - bezesporná, má model $\mathcal{M}$ s $D_{\mathcal{M}} = \{1\}$ a $\alpha_{\mathcal{M}}(.) = \{((1,1),1)\}$
  - není úplná, má model $\mathcal{M}'$ s $D_{\mathcal{M}'} = \{1,2\}$ a $\alpha_{\mathcal{M}'}(.) = \{((1,1),1),((1,2),2)),((2,1),1),((2,2),1)\}$ kde pro $\psi = \exists x(x.x \neq x)$ je $\mathcal{M} \not\models \neg\psi$ ale $\mathcal{M}' \models \psi$.
* $T_2 = \{\varphi_1, \varphi_2\}$
  - stále bezesporná ($\mathcal{M}$)
  - uplná, $\mathcal{M}$ je jediný (každá φ v $\mathcal{M}$ platí pozitvní nebo negovaná, a tedy platí pro všechny modely, což se pak z Gö. v. o ú. dá dokázat)
* $T_3 = \{\varphi_1, \varphi_3\}$
  - sporná, obojí nemůže platit zároveň v žádné interpretaci, nemá model
  - každá sporná teorie je i úplná, protože ze sporu je dokazatelné vše

Efektivnost + bezespornost + úplnost $\Rightarrow$ mechanický matematik

Pro efektivní, bezespornou a úplnou teorii existuje program Mechanický matematik, který ověří, jestli je daná formule φ jejím důsledkem:

foreach *řetězec (generováno v abecedím pořadí)* **do**
  if *řetězec* je důkazem φ **then return** $T \models \varphi$
  if *řetězec* je důkazem $\neg\varphi$ **then return** $T \not\models \varphi$

- Důkaz je řetězec symbolů z konečné abecedy symbolů.
- Řetězce je možné generovat v abecedním pořadí, na každý jednou dojde.
- Efektivnost: existuje program, který rozhodne, zda je řetězec důkazem.
- Úplnost: program jednou určitě skončí nalezením důkazu $\neg\varphi$ nebo φ.

Příklad běhu Mecha. matematika: Je $T_{PA} \models S(0) + S(0) = S(S(0))$?

a	
b	$xyp =\rightarrow$
c	$\dots$
$\dots$	$x = y \rightarrow p$
$\wedge$	$\dots$
$\neg$	$xy =\rightarrow (((,((\wedge\neg\neg x,,\exists$
$\exists$	$\dots$
aa	$p\rightarrow((p\rightarrow p)\rightarrow p),\quad (p\rightarrow(p\rightarrow p)\rightarrow(p\rightarrow p)),\quad \forall x\forall y\, x{=}y$
ab	$\dots$
ac	Proletěl mi bobr zdí, myslel, že to ubrzdí. (Plíhal)
$\dots$	$\dots$
aab	$\boldsymbol{p\rightarrow((p\rightarrow p)\rightarrow p),\quad (p\rightarrow((p\rightarrow p)\rightarrow p)\rightarrow((p\rightarrow(p\rightarrow p))\rightarrow(p\rightarrow p)),\quad \underline{(p\rightarrow(p\rightarrow p)\rightarrow(p\rightarrow p))}}$
$\dots$	$\dots$
$ab\exists$	$\dots$
$\dots$	$\dots$
$a \vee b\neg($	**$\forall\neg(S(x){=}0)$..............................důkaz....................................., $\underline{S(0){+}S(0){=}S(S(0))}$**
$\dots$	

K zapamatování

* Teorie
* Model teorie
* Důsledek teorie
* Bezespornost teorie
* Úplnost teorie
* Gödelova věta o úplnosti (dokazatelné v teorii jsou právě důsledky teorie)
* Je bezesporná $\Leftrightarrow$ má model.
* Je úplná $\Leftrightarrow$ nemá „rozlišitelné“ modely.
* Úplná efektivní teorie umožňuje sestrojit mechanického matematika.

Část V

Limity formálních systémů, neúplnost

Dokazování o „zajímavých“ matematických strukturách?

* Mat. struktura je definována úplnou (a bezespornou a efektivní) teorií $\Rightarrow$ všechno se dá dokázat nebo vyvrátit, a existuje mechanický matematik.
* Je to možné pro zajímavé matematické struktury?
  Npř. aritmetika přir. čísel, množiny, relace, algebry, grafy, ...?

Gödelovy věty o neúplnosti

První Gödelova věta o neúplnosti:
Žádná efektivní bezesporná teorie PL zahrnující Peanovu aritm. nemůže být úplná.

* Za první větou stojí lhářův paradox („Teď lžu.“). Formule φ: „Jsem nedokazatelná.“
* V T_{PA} nemůžeme dokázat všechny teorémy o aritmetice přirozených čísel. T_{PA} nedefinuje přirozená čísla úplně přesně.
* Nejde to opravit, v PL ani a v žádném jiném efektivním bezesporném systému.
* Logické odvozování má své limity, stejně jako počítání.
* Pro aritmetiku přir. čísel se nedá sestrojit dokonalý mechanický matematik.

Příklady teorí: Peanova aritmetika T_{PA}

1. $\forall x \neg(S(x) = 0)$ (nula je první)
2. $\forall xy(S(x) = S(y) \rightarrow x = y)$ (každý má jiného následníka)
3. pro formule φ jazyka T_{PA} s jednou volnou proměnou:

$$\left[\varphi(0) \wedge (\forall x(\varphi(x) \rightarrow \varphi(S(x))))\right] \rightarrow \forall x\,(\varphi(x)) \qquad \text{(ax. indukce)}$$

4. $\forall x(x + 0 = x)$ (0 je neutrální k $+$)
5. $\forall xy(x + S(y) = S(x + y))$ (def sčítání)
6. $\forall x(x \cdot 0 = 0)$ (0 je nulová k $\cdot$)
7. $\forall xy(x \cdot S(y) = x \cdot y + x)$ (def násobení)

$$0, \overset{1}{S}(0), S(\overset{2}{S}(0)), S(S(\overset{3}{S}(0))), S(S(S(\overset{4}{S}(0)))), S(S(S(S(\overset{5}{S}(0))))), \ldots$$

$$T_{PA} \models \overset{1}{S}(0) + \overset{1}{S}(0) = S(\overset{2}{S}(0)) \quad \text{a} \quad T_{PA} \vdash \overset{1}{S}(0) + \overset{1}{S}(0) = S(\overset{2}{S}(0))$$

Gödelovy věty o neúplnosti

Druhá Gödelova věta o neúplnosti:
V žádném bezesporném a efektivním logickém systému zahrnujícím Peanovu aritm. není možné dokázat jeho vlastní bezespornost.


HILBERT
TXS
TOMU
DAL
GÖDEL

Praxe versus teorie

* Bez ohledu na Göelovu neúplnost, formální odvozování/dokazování je jedním ze základních principů moderní matematiky a informatiky, a funguje.
* Velká část informatiky se zabývá mechanizací fragmentů matematiky a mnoho problémů je velmi dobře řešitelných v praxi.